CLAIMS

1. A data processing device for utilizing a digital work recorded on a recording medium having also recorded (i) a plurality of record digest values generated from a plurality of data blocks constituting the digital work and (ii) record signature data generated based on some or all of the plurality of record digest values thereon, comprising:

a using unit operable to use the digital work;

a selecting unit operable to randomly select a predetermined number of data blocks from the plurality of data blocks;

a calculating unit operable to calculate a calculation digest value with respect to each of the selected data blocks;

a reading unit operable to read remaining record digest values, each of which corresponds to one of the unselected data blocks, from among the plurality of record digest values;

a signature verifying unit operable to verify whether the digital work is valid by using the record signature data, the calculation digest values, and the remaining record digest values; and

a use controlling unit operable to stop the using unit from using the digital work when the signature verifying unit judges that the digital work is not valid.

2. The data processing device of Claim 1, wherein

the plurality of record digest values include a plurality of primary record digest values, each of which is generated for

one of the plurality of data blocks, and a plurality of secondary record digest values generated from two or more of the plurality of primary record digest values, and the record signature data is generated by performing a digital signature on the plurality of secondary record digest values,

the reading unit reads the remaining record digest values from among the plurality of primary record digest values, and

the signature verifying unit verifies validity of the digital work by calculating one or more secondary calculation digest values based on the calculation digest values and the remaining record digest values, and performing a digital signature verification with use of the record signature data, the plurality of secondary record digest values, and the secondary calculation digest values.

3. The data processing device of Claim 2, wherein

the digital work includes a plurality of files, each of which corresponds to one of the plurality of secondary record digest values and is constituted by two or more of the plurality of data blocks,

each of the plurality of secondary record digest values is generated by using primary record digest values corresponding one-to-one with the two or more of the plurality of data blocks constituting a file corresponding to the secondary record digest value,

the signature verifying unit includes:

a primary reading subunit operable to read the record signature data from the recording medium;

a calculating subunit operable to calculate a secondary calculation digest value, with respect to each file including at least one of the selected data blocks, by using primary record digest values corresponding to the unselected data blocks included in the file and the calculation digest values corresponding to the selected data blocks;

a secondary reading subunit operable to read, with respect to each file including none of the selected data blocks, a secondary record digest value corresponding to the file;

a signature subunit operable to generate calculation signature data by performing the digital signature with use of the calculated secondary calculation digest values and the read secondary record digest values; and

a comparing subunit operable to compare the calculation signature data and the record signature data, and

the signature verifying unit verifies that the digital work is valid when the calculation signature data and the record signature data conform to each other, and judges that the digital work is not valid when the calculation signature data and the record signature data do not conform to each other.

4. The data processing device of Claim 3, wherein

the plurality of record digest values are hash values each generated by a hash function,

the calculation digest values calculated by the calculating unit are hash values calculated by applying the hash function to each of the selected data blocks, and

the secondary calculation digest values calculated by the

calculating subunit are hash values calculated by applying the hash function to the primary record digest values corresponding to the unselected data blocks and the calculation digest values.

5. The data processing device of Claim 3, wherein

the digital work is digital contents, and the using unit uses the digital contents by playing back the digital contents.

6. The data processing device of Claim 3, wherein

the digital work is a computer program, and the using unit uses the computer program by decrypting instruction codes constituting the computer program and operating according to the decrypted codes.

7. The data processing device of Claim 3, comprising, instead of the use controlling unit:

a warning display unit operable to display, when the digital work is judged as not being valid, a notice of invalidity of the digital work.

8. The data processing device of claim 1 wherein the recording medium has additionally recorded (i) filling contents having an adjusted data size so that capacity of free space on the recording medium becomes a predetermined value or lower and (ii) signature data generated based on part or all of the digital work and the filling contents, the data processing device further comprising:

a verifying unit operable to verify whether the digital

work and the filling contents are valid by using the digital work, the filling contents, and the signature data, and

the use controlling unit operable to stop the using unit from using the digital work when the verifying unit judges that at least one of the digital work and the filling contents is not valid.

9. The data processing device of claim 1 wherein the recording medium has additionally recorded (i) area information indicating an access permitted area, on the recording medium, that an external device is permitted to access and (ii) signature data generated based on part or all of the digital work and the area information, the data processing device further comprising:

an access prohibiting unit operable to prohibit access to areas other than the access permitted area based on the area information; and

a verifying unit operable to verify whether the digital work and the area information are valid by using the digital work, the area information, and the signature data, and

the use controlling unit operable to stop the using unit from using the digital work when the verifying unit judges that at least one of the digital work and the area information is not valid.

10. The data processing device of Claim 1, wherein

the selecting unit, the calculating unit, the reading unit, and the signature verifying unit are assembled together in a

single large scale integration.

11. A recording medium having recorded thereon:

a digital work;

a plurality of digest values generated from a plurality of data blocks constituting the digital work; and

signature data generated based on the plurality of digest values.

12. A data processing method for utilizing a digital work recorded on a recording medium having also recorded (i) a plurality of record digest values generated from a plurality of data blocks constituting the digital work and (ii) record signature data generated based on some or all of the plurality of record digest values thereon, comprising the steps of:

(a) using the digital work;

(b) randomly selecting a predetermined number of data blocks from the plurality of data blocks;

(c) calculating a calculation digest value with respect to each of the selected data blocks;

(d) reading remaining record digest values, each of which corresponds to one of the unselected data blocks, from among the plurality of record digest values;

(e) verifying whether the digital work is valid by using the record signature data, the calculation digest values, and the remaining record digest values; and

(f) stopping the step (a) when the digital work is judged as not being valid in the step (e).

13. A data processing program for utilizing a digital work recorded on a recording medium having also recorded (i) a plurality of record digest values generated from a plurality of data blocks constituting the digital work and (ii) record signature data generated based on some or all of the plurality of record digest values thereon, comprising the steps of:

(a) using the digital work;

(b) randomly selecting a predetermined number of data blocks from the plurality of data blocks;

(c) calculating a calculation digest value with respect to each of the selected data blocks;

(d) reading remaining record digest values, each of which corresponds to one of the unselected data blocks, from among the plurality of record digest values;

(e) verifying whether the digital work is valid by using the record signature data, the calculation digest values, and the remaining record digest values; and

(f) stopping the step (a) when the digital work is judged as not being valid in the step (e).

14. The data processing program of Claim 13 recorded on a computer-readable recording medium.

15. The data processing program of Claim 13 to be transmitted and received via telecommunications.